PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 02 June 1999 (02.06.99)	
International application No. PCT/EP98/06769	**Applicant's or agent's file reference** 22738 WO
International filing date (day/month/year) 24 October 1998 (24.10.98)	**Priority date** (day/month/year) 28 October 1997 (28.10.97)
Applicant RÖVER, Stefan et al	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   05 May 1999 (05.05.99)

   [ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Jean-Marie McAdams

Telephone No.: (41-22) 338.83.38

7/8

VERTRAG ÜBER D[redacted]NTERNATIONALE ZUSAMM[redacted]ARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
22738 WO		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP98/06769	24/10/1998	28/10/1997
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK		
H04L9/32		
Anmelder		
BROKAT INFOSYSTEMS AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 4 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 7 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
05/05/1999	02. 11. 99
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Haas, H Tel. Nr. +49 89 2399 8800

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP98/06769

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-3,7-17	ursprüngliche Fassung			
4-6,6a	eingegangen am	19/10/1999	mit Schreiben vom	18/10/1999

Patentansprüche, Nr.:

1-12	eingegangen am	19/10/1999	mit Schreiben vom	18/10/1999

Zeichnungen, Blätter:

1/3-3/3	ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-12
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-12
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-12
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

SEKTION V

Die internationale Anmeldung betrifft ein Verfahren (Anspruch 1), sowie eine Chipkarte (Anspruch 12), zum digitalen Signieren einer Nachricht.

Der nächstkommende Stand der Technik ist das vom Anmelder genannte Dokument WO-A-96 32700. Dort wird in einem Kommunikationsmodul mit Chipkarte eine Nachricht erzeugt, signiert, und abgeschickt.

Die übrigen Dokumente des internationalen Recherchenberichts beinhalten lediglich einen allgemeineren Stand der Technik im Bezug auf die digitale Signatur von Nachrichten.

Zum standortunabhängigen und leicht realisierbaren Signieren digitaler Nachrichten wird gemäß den Ansprüchen 1 und 12 der internationalen Anmeldung eine zu signierende Nachricht über das Telefonnetz an ein Signiergerät übertragen und dort für die weitere Übertragung signiert.

Dieser Sachverhalt wird durch die Dokumente des internationalen Recherchenberichts weder einzeln noch in Kombination offenbart oder nahegelegt. Neuheit und erfinderische Tätigkeit werden somit anerkannt.

Dies gilt auch bezüglich der abhängigen Ansprüche 2 bis 11.

Die gewerbliche Anwendbarkeit ist für das digitale Signatur in einem Mobilfunksystem ebenfalls gegeben.

mit der Rechner-Tastatur unter Umgehung der Rechner-Software verbunden. Die Signatur wird im Signiergerät erzeugt. Je mehr Aufgaben dabei von der Rechner-Software übernommen werden und je weniger das Signiergerät leisten muss, desto kostengünstiger ist das Verfahren.

Die WO 96/32700 offenbart ein Verfahren gemäß dem eine in einem Mobilfunktelefon erzeugte Nachricht digital signiert und weitergeleitet wird. Die EP 0 689 316 A2 offenbart ein Verfahren und eine Einrichtung zur Identifizierung und Verifizierung von Daten in einem Kommunikationsnetzwerk.

Grundsätzlich besteht in all diesen Ausführungsformen jedoch das Problem, dass genau die Daten signiert werden müssen, die der Benutzer signieren möchte. Es muss also ausgeschlossen werden, dass ein Virus beispielsweise die Daten während der Übertragung von der Darstellungskomponente, zum Beispiel dem Display, an die Signierkomponente, zum Beispiel den Kryptoprozessor, verändert. Ferner muss sichergestellt werden, dass eine Geheimzahl (zum Beispiel PIN), die zur Auslösung der Signaturen notwendig ist, nicht von anderen Programmen von der Tastatur mitgelesen werden kann und Dritten bekannt wird.

Zudem wird der möglichst flächendeckende Einsatz der Möglichkeit zur digitalen Signatur durch die vergleichsweise geringe Verbreitung von Signiergeräten eingeschränkt. In potentiellen Anwendungsbereichen digitaler Signaturen, wie beispielsweise dem Internet-Banking, müsste demgemäss eine kosten

aufwendige Infrastruktur zur Verbreitung der Signiergeräte geschaffen werden. Problematisch ist dabei auch die Installation von Signiergeräten am Rechner. Einerseits müssen die Geräte physikalisch mit dem Rechner verbunden werden, wobei die seriellen Schnittstellen eines PC häufig bereits belegt sind. Alternative Verfahren zur Anbindung der Signiergeräte an Rechner sind ebenfalls problematisch, da hierfür zumindest die Installation von Software-Treibern und manchmal auch von zusätzlicher Hardware notwendig ist. Zusätzlich müssen für alle Signiergeräte häufig spezielle Software-Komponenten installiert werden, die es dem Anwendungsprogramm erlauben, mit dem Signiergerät zu kommunizieren.

Ein weiteres Problem der herkömmlichen Verfahren zur digitalen Signatur besteht darin, dass diese standortabhängig sind. Bestimmte Anwendungsbereiche für den Einsatz digitaler Signaturen, wie beispielsweise das Internet-Banking, sind aufgrund überall zugänglicher öffentlicher Internet-Terminals standortunabhängig. Würden diese Internet-Banking-Anwendungen nun mit den bekannten standortabhängigen Verfahren zur digitalen Signatur kombiniert werden, wäre die Standortunabhängigkeit dieser Anwendungsbereiche verloren.

Das der vorliegenden Erfindung zugrundeliegende technische Problem besteht also darin, ein kostengünstiges, leicht zu realisierendes und standortunabhängiges Verfahren zum digitalen Signieren von Nachrichten sowie dafür geeignete Vorrichtungen bereitzustellen.

Dieses technische Problem wird durch die Lehre gemäß Hauptanspruch gelöst. Die Erfindung sieht demgemäss ein Verfahren zum digitalen Signieren einer an eine Empfangsvorrichtung zu übertragenden Nachricht mittels eines Signiergerätes vor, wobei die zu signierende Nachricht von einer Sendevorrichtung an eine Empfangsvorrichtung, diese Nachricht anschließend von der Empfangsvorrichtung über ein Telefonnetz, insbesondere ein Mobilfunktelefonnetz, an ein der Sendevorrichtung zugeordnetes Signiergerät übertragen wird, diese Nachricht sodann im Signiergerät signiert und an die Empfangsvorrichtung als signierte Nachricht zurückübertragen wird. In besonders bevorzugter Ausführungsform der Erfindung ist das Signiergerät ein Mobilfunktelefon und das Telefonnetz dementsprechend das Mobilfunktelefonnetz.

Im Zusammenhang mit der vorliegenden Erfindung wird unter einem digitalen Signieren einer Nachricht ein Vorgang verstanden, bei dem auf elektronischem Wege der Wille zur Abgabe und der Inhalt einer Nachricht bestätigt wird. Dies geschieht durch partielle oder vollständige Verschlüsselung der zu signierenden Nachricht oder durch Verschlüsselung einer kryptographischen Prüfsumme dieser Nachricht in eine signierte Nachricht mittels eines geheimen Schlüssels unter Anwendung eines mathematischen Verfahrens. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer signierten Nachricht entweder die signierte Nachricht als ganze oder die Signatur selbst verstanden. Die Signierung dient dazu, später eine Authentifizierung des Nutzers durchführen

zu können. Im Zusammenhang mit der vorliegenden Erfindung wird also unter einer signierten Nachricht auch nur die elektronisch erzeugte Signatur der Nachricht verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer Nachricht jegliche Art von in elektronischer Form wiedergebbarer Information, beispielweise Zahlen, Buchstaben, Zahlenkombinationen, Buchstabenkombinationen, Grafiken, Tabellen etc. verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einem Signiergerät eine Einheit verstanden, die eine Si-

PCT/EP98/06769 22738 SC-ne
Anm.: BROKAT INFOSYSTEMS AG.... 18. Oktober 1999

Ansprüche

1. Verfahren zum digitalen Signieren einer an eine Empfangsvorrichtung zu übertragenden Nachricht mittels eines Signiergeräts, **dadurch gekennzeichnet,** dass die zu signierende Nachricht (3) von einer Sendevorrichtung (1) an eine Empfangsvorrichtung (5), diese Nachricht anschließend von der Empfangsvorrichtung (5) über ein Telefonnetz an ein der Sendevorrichtung (1) zugeordnetes Signiergerät übertragen wird, diese Nachricht sodann im Signiergerät signiert und an die Empfangsvorrichtung (5) als signierte Nachricht (9) zurückübertragen wird.

2. Verfahren nach Anspruch 1, wobei das Signiergerät ein Mobilfunktelefon (7) ist.

3. Verfahren nach Anspruch 2, wobei das Telefonnetz ein Mobilfunktelefonnetz ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Signierung ein Public-Key-Verfahren eingesetzt wird, insbesondere ein Public-Key-Verfahren, bei dem die Sendevorrichtung (1) über

einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung (5) über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachrichten zwischen Empfangsvorrichtung (5) und Mobilfunktelefon (7) mittels des Short-Message-Service (SMS) übertragen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht (3) vor der Signierung mittels einer im Mobilfunktelefon (7) vorgesehenen Anzeigeeinrichtung (13) dargestellt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel über eine Tastatureinrichtung des Mobilfunktelefons (7) eingegeben wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons (7) abgelegt ist, und dieser Schlüssel mittels einer über eine Tastatureinrichtung des Mobilfunktelefons (7) eingebbaren Geheimzahl (PIN) freigegeben wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Chip-Karte die Erstellung der signierten Nachricht (9) durchführt.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon (7) die Erstellung der signierten Nachricht (9) durchführt und wobei der geheime Schlüssel aus der Chip-Karte (25) gelesen wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon (7) zusätzlich als Sender zur Übermittlung der signierten Nachricht (9) an die Empfangsvorrichtung (5) dient.

12. Chip-Karte für ein Mobilfunktelefon, wobei die Chip-Karte (25) eine Signiervorrichtung (21) umfaßt, die eine Speichereinheit (27) zur Speicherung des für die Erstellung der signierten Nachricht (9) notwendigen geheimen Schlüssels aufweist, **dadurch gekennzeichnet, dass** die Signiervorrichtung (21) aus einer vom Mobilfunktelefon (7) über das Telefonnetz empfangenen zu signierenden Nachricht (3) eine signierte Nachricht (9) erstellt.

Gleiss & Große
Patentanwälte

Dr. jur. Alf-Olav Gleiss, Dipl.-Ing.
Rainer Große, Dipl.-Ing.
Dr. Frhr. v. Uexküll, Dipl.-Chem.
Michael Lindner, Dipl.-Ing.
Dr. Andreas Schrell, Dipl.-Biol.

European Patent Attorneys
European Trademark Attorneys

70469 **STUTTGART**
MAYBACHSTRASSE 6A
Telefon: (0711) 81 45 55
Telefax: (0711) 81 30 32
Telex: 72 27 72 jura d
e-mail: jurapat@aol.com

*22609 **HAMBURG**
KÖNIGGRÄTZSTRASSE 8
Telefon: (040) 80 33 97
Telefax: (040) 80 52 47

In Zusammenarbeit mit:
Patentanwalt Dipl.-Ing.
Henry Schneider, Berlin

Patentanmeldung

Verfahren zum digitalen Signieren einer Nachricht

BROKAT Informationssysteme GmbH
Hans-Klemm-Straße 5

D-71034 Böblingen

Gleiss & Große
Patentanwälte
Stuttgart Hamburg

3/PRTS

Verfahren zum digitalen Signieren einer Nachricht

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum digitalen Signieren einer Nachricht sowie die zur Durchführung dieses Verfahrens benötigten Vorrichtungen.

Digitale Signaturen, also elektronische Unterschriften, werden üblicherweise mit Hilfe von sogenannten Public-Key-Verfahren realisiert. Dabei wird einem Signierer ein Schlüsselpaar zugeordnet, das einen geheimen und einen öffentlichen Schlüssel umfaßt. Mittels des geheimen Schlüssels wird durch ein mathematisches Verfahren eine Signatur erzeugt, während mit dem zugehörigen öffentlichen Schlüssel diese Signatur überprüft werden kann. Der geheime Schlüssel steht ausschließlich unter der Kontrolle des Signierers, so daß niemand im Namen des Signierers unterschreiben kann. Der öffentliche Schlüssel hingegen kann veröffentlicht werden, so daß jeder die Signatur prüfen kann. In der Regel wird der geheime Schlüssel über ein Kennwort (PIN) geschützt, so daß zur Durchführung einer Signatur das Wissen über das Kennwort und der Besitz des geheimen Schlüssels notwendig sind.

Digitale Signaturen können in einem Rechner, zum Beispiel in einem PC, mit Hilfe von Software-

Programmen erzeugt werden. Üblicherweise wird dabei der zugehörige geheime Schlüssel auf einer Festplatte oder einer Diskette gespeichert und zur Erzeugung der Signatur in den Hauptspeicher geladen. Meistens wird der geheime Schlüssel selbst wiederum in verschlüsselter Form gespeichert und über ein Kennwort geschützt, welches der Eigentümer beim Signieren über die Software angeben muß. So soll sichergestellt werden, daß nur der Inhaber des geheimen Schlüssels diesen auch zum Signieren verwenden kann. Da keine zusätzliche Hardware benötigt wird, ist dieses Verfahren kostengünstig. Als Nachteil erweist sich, daß sich der Benutzer auf die Integrität der Signatur-Software verlassen muß und diese im allgemeinen als nicht ausreichend sicher angesehen wird.

Als weitere Alternative zur Erzeugung von digitalen Signaturen in einem Rechner dienen Hardware-basierte Verfahren. Diese verwenden zum Signieren spezialisierte Geräte, bei denen die Darstellungskomponente und die Tastatur per Hardware so mit der Signierkomponente gekoppelt sind, daß auf die Verbindung kein Einfluß genommen werden kann. Diese Geräte werden in der Regel über eine galvanische Verbindung, beispielsweise ein Kabel zur seriellen Schnittstelle, mit dem Rechner verbunden. Diese Geräte verfügen über eine eigene Darstellungskomponente, die die zu signierende Nachricht anzeigt und über eine eigene Tastatur, das sogenannte PIN-Pad, über welche das Kenntwort zum Freischalten des Schlüssels eingegeben wird. Üblicherweise wird der geheime Schlüssel nicht im Signiergerät gespei-

chert, sondern auf einer Chip-Karte, die in das Gerät eingeführt werden kann. Die eigentliche Signatur kann auf der Chip-Karte erzeugt werden (bei Chip-Karten mit eigenem Kryptoprozessor) oder aber im Gerät. Das beschriebene Hardware-basierte Verfahren stellt ein abgeschlossenes Signiersystem aus Darstellungskomponente, Tastatur, Lesegerät und Chip-Karte dar.

Im Unterschied zu den Software-basierten Verfahren sind Hardware-basierte Verfahren erheblich sicherer, wobei jedoch deren Kosten höher sind. Demgemäß werden gegenwärtig sogenannte gemischte Verfahren eingesetzt. Dabei werden die geheimen Schlüssel meistens auf einer Chip-Karte gespeichert und über ein Lesegerät verfügbar gemacht. Die übrigen Aufgaben wie Darstellung, Eingabe des Kennworts und Erzeugung der Signatur erfolgen ganz oder teilweise im Rechner. Dabei kann vorgesehen sein, daß das Signiergerät, das heißt der Leser und die Chip-Karte, als reines Speichermedium für den geheimen Schlüssel verwendet wird, während die Darstellung, die Eingabe des Kennwortes und die Erzeugung der Signatur vollständig im Rechner erzeugt werden.

Alternativ kann vorgesehen sein, die Darstellung und die Eingabe des Kennwortes über den Rechner erfolgen zu lassen, wobei das Signiergerät zusätzlich zur Speicherung des geheimen Schlüssels auch zur Erzeugung der Signatur verwendet wird. Schließlich existiert die Variante, daß nur die Darstellung im Rechner erfolgt. Das Signiergerät verfügt in dieser Variante über eine eigene Tastatur oder ist direkt

mit der Rechner-Tastatur unter Umgehung der Rechner-Software verbunden. Die Signatur wird im Signiergerät erzeugt. Je mehr Aufgaben dabei von der Rechner-Software übernommen werden und je weniger das Signiergerät leisten muß, desto kostengünstiger ist das Verfahren.

Grundsätzlich besteht in all diesen Ausführungsformen jedoch das Problem, daß genau die Daten signiert werden müssen, die der Benutzer signieren möchte. Es muß also ausgeschlossen werden, daß ein Virus beispielsweise die Daten während der Übertragung von der Darstellungskomponente, zum Beispiel dem Display, an die Signierkomponente, zum Beispiel den Kryptoprozessor, verändert. Ferner muß sichergestellt werden, daß eine Geheimzahl (zum Beispiel PIN), die zur Auslösung der Signaturen notwendig ist, nicht von anderen Programmen von der Tastatur mitgelesen werden kann und Dritten bekannt wird.

Zudem wird der möglichst flächendeckende Einsatz der Möglichkeit zur digitalen Signatur durch die vergleichsweise geringe Verbreitung von Signiergeräten eingeschränkt. In potentiellen Anwendungsbereichen digitaler Signaturen, wie beispielsweise dem Internet-Banking, müßte demgemäß eine kostenaufwendige Infrastruktur zur Verbreitung der Signiergeräte geschaffen werden. Problematisch ist dabei auch die Installation von Signiergeräten am Rechner. Einerseits müssen die Geräte physikalisch mit dem Rechner verbunden werden, wobei die seriellen Schnittstellen eines PC häufig bereits belegt sind. Alternative Verfahren zur Anbindung der Si-

gniergeräte an Rechner sind ebenfalls problematisch, da hierfür zumindest die Installation von Software-Treibern und manchmal auch von zusätzlicher Hardware notwendig ist. Zusätzlich müssen für alle Signiergeräte häufig spezielle Software-Komponenten installiert werden, die es dem Anwendungsprogramm erlauben, mit dem Signiergerät zu kommunizieren.

Ein weiteres Problem der herkömmlichen Verfahren zur digitalen Signatur besteht darin, daß diese standortabhängig sind. Bestimmte Anwendungsbereiche für den Einsatz digitaler Signaturen, wie beispielsweise das Internet-Banking, sind aufgrund überall zugänglicher öffentlicher Internet-Terminals standortunabhängig. Würden diese Internet-Banking-Anwendungen nun mit den bekannten standortabhängigen Verfahren zur digitalen Signatur kombiniert werden, wäre die Standortunabhängigkeit dieser Anwendungsbereiche verloren.

Das der vorliegenden Erfindung zugrundeliegende technische Problem besteht also darin, ein kostengünstiges, leicht zu realisierendes und standortunabhängiges Verfahren zum digitalen Signieren von Nachrichten sowie dafür geeignete Vorrichtungen bereitzustellen.

Dieses technische Problem wird durch die Lehre gemäß Hauptanspruch gelöst. Die Erfindung sieht demgemäß ein Verfahren zum digitalen Signieren einer über ein Kommunikationsnetz an ein Signiergerät übertragenen zu signierenden Nachricht vor, wobei

die zu signierende Nachricht mittels eines Telefonnetzes an ein Signiergerät übertragen wird. In besonders bevorzugter Ausführungsform der Erfindung ist das Signiergerät ein Mobilfunktelefon und das Kommunikationsnetz dementsprechend das Mobilfunknetz.

Im Zusammenhang mit der vorliegenden Erfindung wird unter einem digitalen Signieren einer Nachricht ein Vorgang verstanden, bei dem auf elektronischem Wege der Wille zur Abgabe und der Inhalt einer Nachricht bestätigt wird. Dies geschieht durch partielle oder vollständige Verschlüsselung der zu signierenden Nachricht oder durch Verschlüsselung einer kryptographischen Prüfsumme dieser Nachricht in eine signierte Nachricht mittels eines geheimen Schlüssels unter Anwendung eines mathematischen Verfahrens. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer signierten Nachricht entweder die signierte Nachricht als ganze oder die Signatur selbst verstanden. Die Signierung dient dazu, später eine Authentifizierung des Nutzers durchführen zu können. Im Zusammenhang mit der vorliegenden Erfindung wird also unter einer signierten Nachricht auch nur die elektronisch erzeugte Signatur der Nachricht verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer Nachricht jegliche Art von in elektronischer Form wiedergebbarer Information, beispielweise Zahlen, Buchstaben, Zahlenkombinationen, Buchstabenkombinationen, Grafiken, Tabellen etc. verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einem Signiergerät eine Einheit verstanden, die eine Si-

gnierung einer Nachricht durchführen kann, das heißt einen geheimen Schlüssel, ein mathematisches Verschlüsselungsverfahren, Dialogmöglichkeiten mit dem Signierer oder Nutzer, gegebenenfalls notwendigen Schnittstellen und eine Sende- und Empfangsvorrichtung aufweist. Diese Einheit kann aus verschiedenen Elementen, zum Beispiel aus einer Chip-Karte und einem Lesegerät oder einer Chip-Karte und einem Mobilfunktelefon, aufgebaut sein. Eine Signiervorrichtung ist im Zusammenhang mit der vorliegenden Erfindung eine Komponente des Signiergeräts, die den geheimen Schlüssel und/oder das Verschlüsselungsverfahren und/oder eine Schnittstelle zu beiden oder einer der vorgenannten Komponenten aufweist.

Aufgrund der erfindungsgemäß besonders bevorzugten Verwendung des Funktelefonnetzes zur Übertragung der zu signierenden Nachrichten an ein Signiergerät, das in vorteilhafter Ausgestaltung als Mobilfunktelefon ausgeführt ist, ist es möglich, von einem handelsüblichen Rechner mit Anschluß an einen entsprechenden Nachrichten-Server, zum Beispiel via e-Mail, Nachrichten an das Signiergerät zu übermitteln, ohne am Rechner selbst Installationen oder andere Veränderungen vornehmen zu müssen.

In besonders bevorzugter Ausführungsform sieht die Erfindung ein Verfahren der vorgenannten Art vor, wobei die zu signierende Nachricht von einer auch als Nachrichtenquelle zu bezeichnenden Sendevorrichtung, beispielsweise einem PC, an eine Empfangsvorrichtung, beispielsweise einen Nachrichten-

Server, übertragen wird, anschließend diese Nachricht von der Empfangsvorrichtung an ein der Sendevorrichtung zugeordnetes Signiergerät, insbesondere Mobilfunktelefon übertragen wird, anschließend diese Nachricht im Mobilfunktelefon signiert wird, und sodann an die Empfangsvorrichtung als Signatur, das heißt als signierte Nachricht, zurückübertragen wird.

Die Erfindung sieht also vor, daß von einer Nachrichtenquelle eine unsignierte bzw. zu signierende Nachricht an eine Empfangsvorrichtung, zum Beispiel einen Nachrichten-Server, übertragen wird. Die Empfangsvorrichtung nimmt dann eine Zuordnung der zu signierenden Nachricht zu dem Signiergerät, insbesondere dem Mobiltelefon, vor. Dies geschieht entweder durch eine in der Empfangsvorrichtung hinterlegte Dokumentation oder über Informationen, die zusammen mit der zu signierenden Nachricht von der Sendevorrichtung an die Empfangsvorrichtung übertragen wurde. Die Zuordnung des Signiergeräts, vorteilhafterweise des Mobilfunktelefons, zu der Nachrichtenquelle braucht also keine räumliche Zuordnung zu sein, sondern ist eine rein informatorische Zuordnung. Die Zuordnung besteht also darin, festzustellen, welches Signiergerät und damit welcher Nutzer die empfangene, zu signierende Nachricht signieren soll. Das in bevorzugter Ausführungsform der Erfindung eingesetzte Mobilfunktelefon ist in vorteilhafter Weise in der Lage, eine zu signierende Nachricht darzustellen und auf Anweisung des Nutzers und unter Zuhilfenahme der in vorteilhafter Weise eingesetzten Chip-Karte zu signieren. Die auf

diese Weise signierte Nachricht wird der Empfangsvorrichtung übermittelt und dort gegebenenfalls mit der ursprünglichen Nachricht verglichen und authentifiziert. Von der Empfangsvorrichtung wird die signierte und gegebenenfalls authentifizierte Nachricht dann an einen Adressaten weitervermittelt.

Die Erfindung betrifft auch ein vorgenanntes Verfahren, wobei in vorteilhafter Weise vorgesehen ist, zum Signieren ein Public-Key-Verfahren einzusetzen, bei dem die Sendevorrichtung über einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt. Diese Vorgehensweise bietet den Vorteil, daß die Schlüssel nicht übermittelt werden müssen.

In einer weiteren vorteilhaften Ausgestaltung betrifft die Erfindung ein vorgenanntes Verfahren, wobei die zu signierende Nachricht oder die bereits signierte Nachricht, das heißt zum Beispiel die Signatur zwischen Empfangsvorrichtung und Signiergerät, insbesondere Mobilfunktelefon, mittels des Short-Message-Service (SMS) übertragen werden. In besonders bevorzugter Ausführungsform kann vorgesehen sein, daß sowohl die Übertragung der zu signierenden Nachricht von der Empfangsvorrichtung zum Mobilfunktelefon als auch die Übertragung der signierten Nachricht bzw. der Signatur vom Mobilfunktelefon zur Empfangsvorrichtung mittels des SMS durchgeführt wird.

Die Erfindung sieht in einer weiteren Ausführungsform vor, daß die zu signierende Nachricht mittels einer im Mobilfunktelefon vorgesehenen Anzeigeeinrichtung dargestellt wird. Dies kann auf dem Display handelsüblicher Mobilfunktelefone geschehen. Auf diese Weise lassen sich ohne weiteres einfache Texte, wie zum Beispiel Banktransaktionen oder sogar einfache Grafiken, darstellen.

Im Anschluß an diese gegebenenfalls vorgesehene Darstellung gibt der Benutzer in einem dafür vorgesehenen Dialog eine entsprechende Anweisung zur Auslösung des Signierens. In besonders bevorzugter Ausführungsform sieht die Erfindung ein Verfahren der vorgenannten Art vor, wobei der zum Signieren notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons abgelegt ist und dieser Schlüssel mittels einer über eine Tastatur des Mobilfunktelefons eingebbaren Geheimzahl (im folgenden PIN genannt) freigegeben wird. In vorteilhafter Weise kann durch eine entsprechende übliche Programmierung des Mobilfunktelefons sichergestellt werden, daß die eingegebene PIN nur auf die Chip-Karte übertragen wird und nicht von außen abgehört werden kann.

In einer weiteren alternativen Ausgestaltung der vorgenannten erfindungsgemäßen Verfahren ist vorgesehen, daß der zum Signieren notwendige geheime Schlüssel über eine Tastatur des Mobilfunktelefons eingegeben wird.

In einer weiteren bevorzugten Ausführungsform der Erfindung ist vorgesehen, daß in einem der vorgenannten Verfahren der geheime Schlüssel nicht nur auf der Chip-Karte des Mobilfunktelefons gespeichert ist, sondern dort auch das Signieren der Nachricht durchgeführt wird. Damit kann in vorteilhafter Weise sichergestellt werden, daß der geheime Schlüssel auf keinen Fall die Chip-Karte verläßt und damit von Unbefugten verwendet werden kann.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung ist vorgesehen, daß das Mobilfunktelefon nicht nur zum Signieren der Nachricht, sondern zusätzlich auch als Sender zur Übermittlung der signierten Nachricht an die Empfangsvorrichtung eingesetzt wird.

Die Erfindung betrifft auch Vorrichtungen zur Durchführung der vorgenannten Verfahren, insbesondere Mobilfunktelefone und Chip-Karten.

In einer besonders bevorzugten Ausführungsform der Erfindung ist ein Mobilfunktelefon vorgesehen, das eine Tastatur, eine Anzeigevorrichtung und eine Chip-Karten-Einrichtung zum Lesen und/oder Schreiben einer in das Mobilfunktelefon einsteckbaren Chip-Karte umfaßt, wobei zusätzlich eine Signiervorrichtung vorgesehen ist, die beispielsweise zur Kommunikation mit einer erfindungsgemäßen Chip-Karte und/oder zur Erstellung einer signierten Nachricht aus einer zu signierenden Nachicht geeignet ist. In vorteilhafter Weise ist die Signiervor-

richtung mit der Tastatur zur Eingabe eines geheimen Schlüssels oder einer Geheimzahl verbunden.

In besonders vorteilhafter Ausgestaltung des vorgenannten Mobilfunktelefons ist vorgesehen, daß die Signiervorrichtung eine gegenüber der herkömmlichen Softwarekomponente eines Mobilfunktelefons geänderte Softwarekomponente darstellt. Diese geänderte Softwarekomponente ist in einer bevorzugten Ausgestaltung der Erfindung dazu geeignet, das Signieren der Nachricht nach Dialog mit dem Nutzer durchzuführen. In einer weiteren Ausführungsform ist die erfindungsgemäß vorgesehene geänderte Softwarekomponente des Signiergeräts vorteilhafterweise in der Lage, mit der erfindungsgemäßen Chip-Karte zur Durchführung des erfindungsgemäßen Signierens kommunizieren zu können. In besonders vorteilhafter Ausgestaltung der Erfindung ist vorgesehen, daß die Signiervorrichtung des Signiergeräts zusätzlich Algorithmen abarbeiten kann, die die Anzeige der zu signierenden Nachricht im Anzeigefeld des Mobilfunktelefons ermöglichen.

In besonders vorteilhafter Weise stellt die vorliegende Erfindung also ein System zur Verfügung, gemäß dem lediglich Softwarekomponenten gegenüber in herkömmlicher Weise verwendeter Softwarekomponenten zu modifizieren sind. Eine Änderung der Hardware ist nicht notwendig.

In einer weiteren Ausgestaltung der Erfindung betrifft die Erfindung auch Chip-Karten für Mobilfunktelefone, insbesondere für die vorgenannten Mo-

bilfunktelefone, wobei die Chip-Karte eine Signiervorrichtung umfaßt, die den geheimen Schlüssel des Nutzers speichern kann. In vorteilhafter Weise ist die Signiervorrichtung der Chip-Karte darüber hinaus in der Lage, aus einer vom Mobilfunktelefon empfangenen Nachricht, das heißt einer zu signierenden Nachricht, eine signierte Nachricht zu erstellen. Im Zusammenhang mit der vorliegenden Erfindung wird unter der Signiervorrichtung einer erfindungsgemäßen Chip-Karte also eine Vorrichtung verstanden, die den geheimen Schlüssel des Nutzers speichert, und in vorteilhafter Ausgestaltung auch das Signieren durchführt. Die Durchführung des Signierens muß jedoch nicht unmittelbar auf der Chip-Karte, sondern kann durch eine Software- und/oder Hardwarekomponente im Mobilfunktelefon erfolgen.

Weitere vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen.

Die Erfindung wird anhand der Figuren sowie des dazugehörigen Ausführungsbeispiels näher erläutert.

Die Figuren zeigen:

Figur 1 stellt den Ablauf des erfindungsgemäßen Verfahrens,

Figur 2 in schematischer Weise den Aufbau eines erfindungsgemäßen Mobilfunktelefons und

Figur 3 eine schematische Darstellung einer erfindungsgemäßen Chip-Karte dar.

Die Figur 1 stellt die Sendevorrichtung 1, die in Form eines einen Texteditor oder ein Homebanking-Programm aufweisenden PCs ausgeführt sein kann, eine zu signierende Nachricht 3, eine Empfangsvorrichtung 5, die in Form eines Nachrichten-Servers ausgeführt ist, ein Mobilfunktelefon 7, eine signierte Nachricht 9 und einen Adressaten 11 dar.

Mittels eines in der Sendevorrichtung 1 enthaltenen Homebanking-Programms wird eine zu signierende Nachricht 3, beispielsweise per e-Mail an die Empfangsvorrichtung 5 gesendet. Die Empfangsvorrichtung 5 wandelt die empfangene zu signierende Nachricht 3 in eine Nachricht um, die an das Mobilfunktelefon 7 gesendet werden kann, insbesondere mittels eines Mobilfunknetzes, in vorteilhafter Ausgestaltung mittels des SMS. Die Empfangsvorrichtung 5 ordnet die zu signierende Nachricht 3 dem Mobilfunktelefon 7, beispielsweise mittels einer in der Empfangsvorrichtung 5 hinterlegten Information, zu. Es kann auch vorgesehen sein, daß die Zuordnung mittels einer von der Sendevorrichtung 1 zusammen mit der zu signierenden Nachricht 3 übermittelten Information erfolgt. Bei dieser Information handelt es sich im allgemeinen um die Mobilfunktelefonnummer.

Im Mobilfunktelefon 7 wird die empfangene Nachricht 3 in einer Anzeigeeinrichtung 13 dargestellt. Die genaue Verfahrensweise wird in der Beschreibung zu Figur 2 näher erläutert. Nach Anzeige der zu signierenden Nachricht 3 in der Anzeigeeinrichtung 13

wird die zu signierende Nachricht 3 auf Anweisung des Benutzers signiert und die signierte Nachricht 9 an die Empfangsvorrichtung 5 oder auch an einen anderen Empfänger weitervermittelt. Die Übertragung der signierten Nachricht 9 vom Mobilfunktelefon 7 zur Empfangsvorrichtung 5 geschieht ebenfalls mittels SMS. Die Empfangsvorrichtung 5 kann die signierte Nachricht 9 mit der ursprünglichen zu signierenden Nachricht 3 vergleichen und anschließend an einen Adressaten 11 übermitteln. Die Übermittlung an den Adressaten 11 kann auf beliebigem Wege erfolgen.

Die Figur 2 stellt ein Mobilfunktelefon 7 dar. Das Mobilfunktelefon 7 umfaßt eine Anzeigeeinrichtung 13, eine Sende- und Empfangseinrichtung 15, eine Chip-Karten-Einrichtung 17, eine Tastatureinrichtung 19 und eine Signiervorrichtung 21.

Die von der Empfangsvorrichtung 5 übersandte zu signierende Nachricht 3 wird von der Sende- und Empfangseinrichtung 15 des Mobilfunktelefons 7 empfangen und gegebenenfalls aufbereitet an die Signiervorrichtung 21 weitergeleitet. Die Signiervorrichtung 21 sorgt für die interne Verwaltung des Signaturablaufs. Die Signiervorrichtung 21 enthält Softwarekomponenten zur Ansteuerung der Anzeigeeinrichtung 13, so daß die zu signierende Nachricht 3 visualisiert werden kann. Weiterhin wird die zu signierende Nachricht 3 innerhalb der Signiervorrichtung 21 signiert. Um den Signiervorgang durchführen zu können, muß die Signiervorrichtung 21 mit der Chip-Karten-Einrichtung 17 kommunizieren. Weiterhin

ist es notwendig, daß die Signiervorrichtung 21 über die Tastatureinrichtung 19 entweder den geheimen Schlüssel direkt oder die PIN übermittelt bekommt. Wird über die Tastatureinrichtung 19 vom Benutzer die PIN eingegeben, die in der Regel kürzer ist, also weniger Stellen umfaßt als der geheime Schlüssel, so kann die PIN mittels eines Betriebssystems einer Chip-Karte 25 den unhandlichen geheimen Schlüssel für den Signiervorgang quasi freigeben. Über eine bidirektional ausgelegte Verbindungsleitung 23 kann die Signiervorrichtung 21 mit der Chip-Karte 25 kommunizieren. Die Chip-Karten-Einrichtung 27 trägt dafür Sorge, daß die Befehle oder Kommandos der Signiervorrichtung 21 ausgeführt werden und die signierte Nachricht 9 über die Signiervorrichtung 21 an die Sende- und Empfangseinrichtung 15 weitergegeben wird. Das heißt, die Chip-Karten-Einrichtung 27 stellt eine Schnittstelle zwischen Signiervorrichtung 21 und der Chip-Karte 25 dar.

Die Figur 3 stellt in sehr vereinfachter schematischer Darstellung eine erfindungsgemäße Chip-Karte 25 dar. Diese umfaßt im wesentlichen ein Kontaktierpad 31 sowie eine Speichereinheit 27 und ein Kryptographiemodul 29. In der Speichereinheit 27 ist der für die Erstellung der signierten Nachricht 9 notwendige geheime Schlüssel abgelegt. Das Kryptographiemodul 29 dient der Verschlüsselung der zu signierenden Nachricht 3, beispielsweise mittels eines RSA-Verfahrens. Über das Kontaktierpad 31 kann die Speichereinheit 27 bzw. das Kryptographiemodul 29 mit der Chip-Karten-Einrichtung 27 in kom-

munikativer Verbindung stehen. Aus Gründen der Übersichtlichkeit sind weitere, für den Betrieb der Chip-Karte 25 notwendige Elemente wie beispielsweise ein Controller in der Darstellung der Figur 3 nicht dargestellt.

Gleiss & Große
Patentanwälte
Stuttgart Hamburg

Ansprüche

1. Verfahren zum digitalen Signieren einer über ein Kommunikationsnetzwerk an ein Signiergerät übertragenen und zu signierenden Nachricht, wobei die zu signierende Nachricht mittels eines Telefonnetzes an das Signiergerät übertragen wird.

2. Verfahren nach Anspruch 1, wobei das Signiergerät ein Mobilfunktelefon ist.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei die zu signierende Nachricht von einer Sendevorrichtung an eine Empfangsvorrichtung, diese Nachricht anschließend von der Empfangsvorrichtung über ein Telefonnetz, insbesondere ein Mobilfunktelefonnetz, an ein der Sendevorrichtung zugeordnetes Mobilfunktelefon übertragen wird, diese Nachricht sodann im Mobilfunktelefon signiert und an die Empfangsvorrichtung als signierte Nachricht zurückübertragen wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Signierung ein Public-Key-Verfahren

eingesetzt wird, insbesondere ein Public-Key-Verfahren, bei dem die Sendevorrichtung über einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachrichten zwischen Empfangsvorrichtung und Mobilfunkttelefon mittels des Short-Message-Service (SMS) übertragen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht vor der Signierung mittels einer im Mobilfunktelefon vorgesehenen Anzeigeeinrichtung dargestellt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel über eine Tastatureinrichtung des Mobilfunktelefons eingegeben wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons abgelegt ist, und dieser Schlüssel mittels einer über eine Tastatureinrichtung des Mobilfunktelefons

eingebbaren Geheimzahl (PIN) freigegeben wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Chip-Karte die Erstellung der signierten Nachricht durchführt.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon die Erstellung der signierten Nachricht durchführt und wobei der geheime Schlüssel aus der Chip-Karte gelesen wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon zusätzlich als Sender zur Übermittlung der signierten Nachricht an die Empfangsvorrichtung dient.

12. Mobilfunktelefon mit einer Tastatur, einer Anzeigevorrichtung und einer Chip-Karten-Einrichtung zum Lesen und/oder Schreiben einer in das Mobilfunktelefon einsteckbaren Chip-Karte, **gekennzeichnet durch** eine Signiervorrichtung (21), insbesondere zur Erstellung einer signierten Nachricht (9) aus einer zu signierenden Nachricht (3) oder/und zur Kommunikation mit einer eine Signiervorrichtung (21) aufweisenden Chip-Karte (25).

13. Mobilfunktelefon nach Anspruch 12, **dadurch gekennzeichnet, daß** die Signiervorrichtung (21) mit

der Tastatureinrichtung (19) zur Eingabe eines geheimen Schlüssels oder einer Geheimzahl verbunden ist.

14. Chip-Karte für ein Mobilfunktelefon, insbesondere nach einem der Ansprüche 12 oder 13, **dadurch gekennzeichnet, daß** die Chip-Karte (25) eine Signiervorrichtung (21) umfaßt, die eine Speichereinheit (27) zur Speicherung des für die Erstellung der signierten Nachricht (9) notwendigen geheimen Schlüssels aufweist.

15. Chip-Karte nach Anspruch 14, **dadurch gekennzeichnet, daß** die Chip-Karte (25) eine Signiervorrichtung (21) umfaßt, die aus einer vom Mobilfunktelefon (7) empfangenen zu signierenden Nachricht (3) eine signierte Nachricht (9) erstellt.

Gleiss & Große
Patentanwaltskanzlei
Stuttgart Berlin Hamburg

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum digitalen Signieren einer Nachricht sowie die dazu notwendigen Mittel.

(Figur 1)

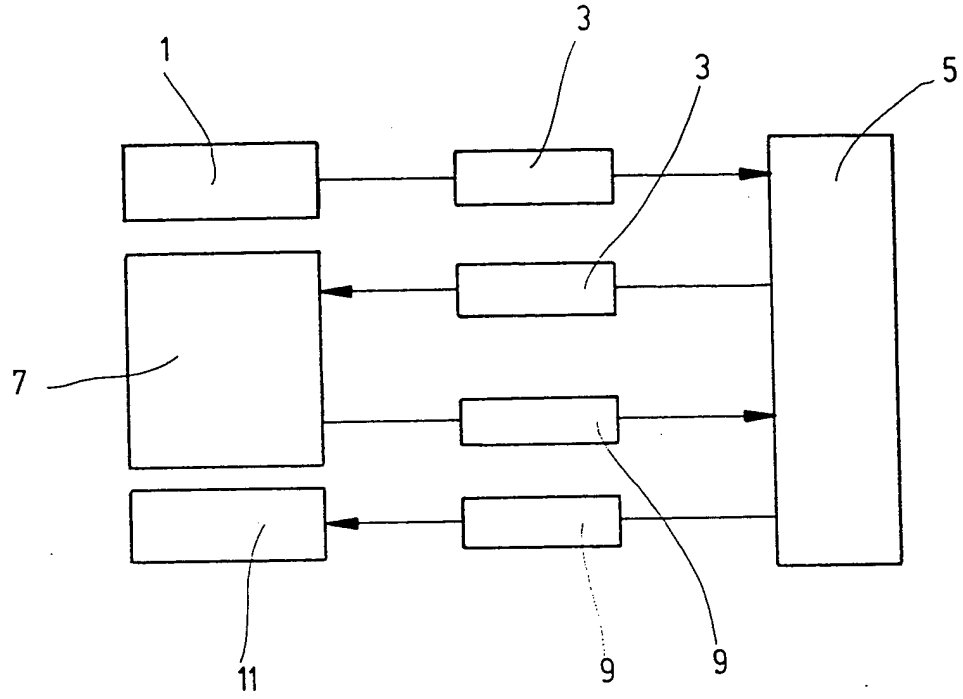

Fig. 1

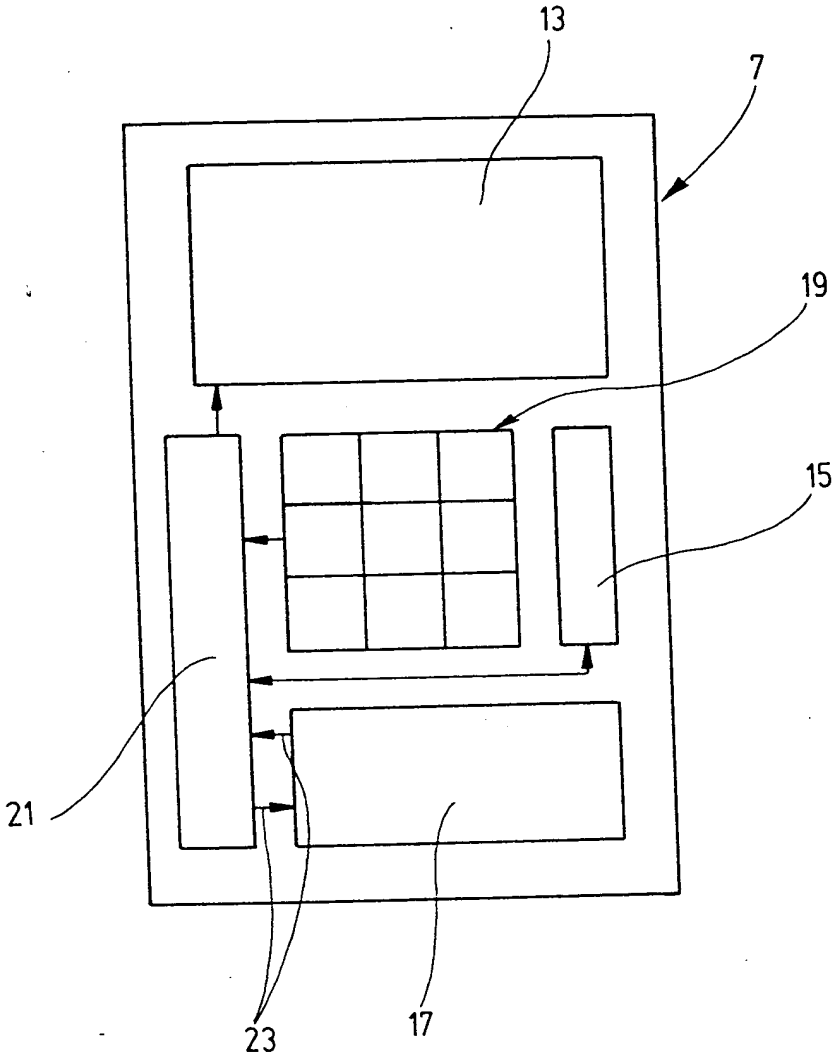

Fig. 2

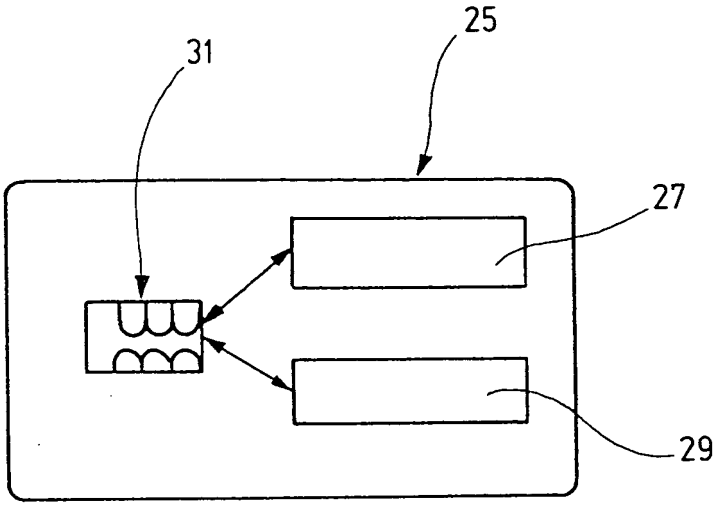

Fig. 3

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

To:
SCHRELL, Andreas
Maybachstrasse 6A
D-70469 Stuttgart
ALLEMAGNE

17. MAI 1999

Bearbeiter: SC/Sch

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

Date of mailing (day/month/year)	
06 May 1999 (06.05.99)	
Applicant's or agent's file reference	**IMPORTANT NOTICE**
22738 WO ✓	

International application No.	International filing date (day/month/year)	Priority date (day/month/year)
PCT/EP98/06769 ✓	24 October 1998 (24.10.98) ✓	28 October 1997 (28.10.97) ✓

Applicant
BROKAT INFOSYSTEMS AG et al ✓

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

   ~~AU~~,CN,~~EP~~,IL,~~JP~~,~~KP~~,~~KR~~,US ✓

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

   ~~AL~~,~~AM~~,~~AP~~,~~AT~~,~~AZ~~,~~BA~~,~~BB~~,~~BG~~,~~BR~~,~~BY~~,~~CA~~,~~CH~~,~~CU~~,~~CZ~~,~~DK~~,~~EA~~,~~EE~~,~~ES~~,FI,GB,~~GE~~,~~GH~~,~~GM~~,~~HR~~,~~HU~~,~~ID~~,~~IS~~,
   ~~KE~~,~~KG~~,~~KZ~~,~~LC~~,~~LK~~,~~LR~~,~~LS~~,~~LT~~,~~LU~~,~~LV~~,~~MD~~,~~MG~~,~~MK~~,~~MN~~,~~MW~~,~~MX~~,~~NO~~,~~NZ~~,~~OA~~,~~PL~~,~~PT~~,~~RO~~,~~RU~~,~~SD~~,~~SE~~,~~SG~~,~~SI~~,
   ~~SK~~,~~SL~~,~~TJ~~,~~TM~~,~~TR~~,~~TT~~,~~UA~~,~~UG~~,~~UZ~~,~~VN~~,~~YU~~,~~ZW~~

   The communication will be made to these Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on

   06 May 1999 (06.05.99) under No. WO 99/22486

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

Continuation of Form PCT/IB/308

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

Date of mailing (day/month/year)	IMPORTANT NOTICE
06 May 1999 (06.05.99)	
Applicant's or agent's file reference	**International application No.**
22738 WO	PCT/EP98/06769

The applicant is hereby notified that, at the time of establishment of this Notice, the time limit under Rule 46.1 for making amendments under Article 19 has not yet expired and the International Bureau had received neither such amendments nor a declaration that the applicant does not wish to make amendments.

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen

Internationales Anmeldedatum

Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)* 22738 WO

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren zum digitalen Signieren einer Nachricht

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

BROKAT Infosystems AG
Industriestraße 3
D-70565 STUTTGART
DE

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Röver, Stefan
Ulmenstraße 20/1
D-71088 HOLZGERLINGEN
DE

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ODER ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☒ Anwalt ☐ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

Schrell, Andreas; Gleiss, Alf-Olav;
Große, Rainer
Maybachstraße 6A
D-70469 STUTTGART
DE

Telefonnr.: 0711/81 45 55

Telefaxnr.: 0711/81 30 32

Fernschreibnr.:

☐ **Zustellanschrift:** Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Blatt Nr. ..2....

Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Wird keines der folgenden Felder benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Groffmann, Hans-Dieter
Birkenstraße 14
D-72145 HIRRLINGEN
DE

Diese Person ist:
☐ nur Anmelder
☒ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

- ☒ AP **ARIPO-Patent:** GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☒ EA **Eurasisches Patent:** AM Armenien, AZ Aserbaidschan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ EP **Europäisches Patent:** AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, CY Zypern, DE Deutschland, DK Dänemark, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☒ OA **OAPI-Patent:** BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

- ☒ AL Albanien
- ☒ AM Armenien
- ☒ AT Österreich
- ☒ AU Australien
- ☒ AZ Aserbaidschan
- ☒ BA Bosnien-Herzegowina
- ☒ BB Barbados
- ☒ BG Bulgarien
- ☒ BR Brasilien
- ☒ BY Belarus
- ☒ CA Kanada
- ☒ CH und LI Schweiz und Liechtenstein
- ☒ CN China
- ☒ CU Kuba
- ☒ CZ Tschechische Republik
- ☐ DE Deutschland
- ☒ DK Dänemark
- ☒ EE Estland
- ☒ ES Spanien
- ☒ FI Finnland
- ☒ GB Vereinigtes Königreich
- ☒ GE Georgien
- ☒ GH Ghana
- ☒ GM Gambia
- ☒ GW Guinea-Bissau
- ☒ HR Kroatien
- ☒ HU Ungarn
- ☒ ID Indonesien
- ☒ IL Israel
- ☒ IS Island
- ☒ JP Japan
- ☒ KE Kenia
- ☒ KG Kirgisistan
- ☒ KP Demokratische Volksrepublik Korea
- ☐ .....
- ☒ KR Republik Korea
- ☒ KZ Kasachstan
- ☒ LC Saint Lucia
- ☒ LK Sri Lanka
- ☒ LR Liberia
- ☒ LS Lesotho
- ☒ LT Litauen
- ☒ LU Luxemburg
- ☒ LV Lettland
- ☒ MD Republik Moldau
- ☒ MG Madagaskar
- ☒ MK Die ehemalige jugoslawische Republik Mazedonien
- ☒ MN Mongolei
- ☒ MW Malawi
- ☒ MX Mexiko
- ☒ NO Norwegen
- ☒ NZ Neuseeland
- ☒ PL Polen
- ☒ PT Portugal
- ☒ RO Rumänien
- ☒ RU Russische Föderation
- ☒ SD Sudan
- ☒ SE Schweden
- ☒ SG Singapur
- ☒ SI Slowenien
- ☒ SK Slowakei
- ☒ SL Sierra Leone
- ☒ TJ Tadschikistan
- ☒ TM Turkmenistan
- ☒ TR Türkei
- ☒ TT Trinidad und Tobago
- ☒ UA Ukraine
- ☒ UG Uganda
- ☒ US Vereinigte Staaten von Amerika
- .....
- ☒ UZ Usbekistan
- ☒ VN Vietnam
- ☒ YU Jugoslawien
- ☒ ZW Simbabwe

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☐ .....
- ☐ .....

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeld*

Feld Nr. VI PRIORITÄTSANSPR ☐ Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.

	Anmeldedatum der früheren Anmeldung *(Tag/Monat)*	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine: national Anmeldung: Staat	regionale Anmeldung:* regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1)	28. Oktober 1997 (28.10.1997)	19747603.1	DE		
Zeile (2)					
Zeile (3)					

☐ Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben in der (den) Zeile(n) _____ bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln *(nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist(sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)*

* *Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, so muß in dem Zusatzfeld mindestens ein Staat angegeben werden, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung eingereicht wurde.*

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA) *(falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden)*

ISA / EP

Antrag auf Nutzung der Ergebnisse einer früheren Recherche; Bezugnahme auf diese frühere Recherche *(falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist):*

Datum *(Tag/Monat/Jahr)* Aktenzeichen Staat *(oder regionales Amt)*

Feld Nr. VIII KONTROLLISTE: EINREICHUNGSSPRACHE

Diese internationale Anmeldung enthält die folgende Anzahl von Blättern:

Antrag	4
Beschreibung (ohne Sequenzprotokollteil)	17
Ansprüche	4
Zusammenfassung	1
Zeichnungen	3
Sequenzprotokollteil der Beschreibung	
Blattzahl insgesamt	29

Dieser internationalen Anmeldung liegen die nachstehend angekreuzten Unterlagen bei:

1. ☒ Blatt für die Gebührenberechnung
2. ☐ Gesonderte unterzeichnete Vollmacht
3. ☐ Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden):
4. ☐ Begründung für das Fehlen einer Unterschrift
5. ☐ Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer gekennzeichnet:
6. ☐ Übersetzung der internationalen Anmeldung in die folgende Sprache:
7. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material
8. ☐ Sequenzprotokolle für Nucleotide und/oder Aminosäuren in computerlesbarer Form
9. ☐ Sonstige *(einzeln aufführen)*:

Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.): 1

Sprache, in der die internationale Anmeldung eingereicht wird: DE

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Dr. Andreas Schrell, European Patent Attorney 23.10.1998

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:	2. Zeichnungen ☐ eingegangen: ☐ nicht eingegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:	
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:	
5. Internationale Recherchenbehörde *(falls zwei oder mehr zuständig sind)*: ISA /	6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Dieses Blatt ist Teil und zählt nicht als Blatt der internationalen Anmeldung.

PCT

BLATT FÜR DIE GEBÜHRENBERECHNUNG

Anhang zum Antrag

Von Anmeldeamt auszufüllen

Internationales Aktenzeichen

Eingangsstempel des Anmeldeamts

Aktenzeichen des Anmelders oder Anwalts: 22738 WO

Anmelder: BROKAT Infosystems AG

BERECHNUNG DER VORGESCHRIEBENEN GEBÜHREN

1. ÜBERMITTLUNGSGEBÜHR . . . . . DM 200,00 [T]
2. RECHERCHENGEBÜHR . . . . . DM 2.200,00 [S]

Die internationale Recherche ist durchzuführen von EP

(Sind zwei oder mehr Internationale Recherchenbehörden für die internationale Recherche zuständig, ist der Name der Behörde anzugeben, die die internationale Recherche durchführen soll.)

3. INTERNATIONALE GEBÜHR

Grundgebühr

Die internationale Anmeldung enthält 29 Blätter.

umfaßt die ersten 30 Blätter . . . . . DM 800,00 [b1]

____ (Anzahl der Blätter über 30) x ____ (Zusatzblattgebühr) = [b2]

Addieren Sie die in Feld b1 und b2 eingetragenen Beträge, und tragen Sie die Summe in Feld B ein . . . . DM 800,00 [B]

Bestimmungsgebühren alle außer

Die internationale Anmeldung enthält DE Bestimmungen.

11 (Anzahl der zu zahlenden Bestimmungsgebühren *(maximal 11)*) x DM 184,00 (Bestimmungsgebühr) = DM 2.024,00 [D]

Addieren Sie die in Feld B und D eingetragenen Beträge, und tragen Sie die Summe in Feld I ein . . . . . DM 2.824,00 [I]

(Anmelder aus einigen Staaten haben Anspruch auf eine Ermäßigung der internationalen Gebühr um 75%. Hat der Anmelder (oder haben alle Anmelder) einen solchen Anspruch, so beträgt der in Feld I einzutragende Gesamtbetrag 25% der Summe der in Feld B und D eingetragenen Beträge.)

4. GEBÜHR FÜR PRIORITÄTSBELEG *(ggf.)* . . . . . [P]
5. GESAMTBETRAG DER ZU ZAHLENDEN GEBÜHREN

Addieren Sie die in Feldern T, S, I und P eingetragenen Beträge, und tragen Sie die Summe in das nebenstehende Feld ein . . . . . DM 5.224,00 INSGESAMT

☐ Die Bestimmungsgebühren werden jetzt noch nicht gezahlt.

ZAHLUNGSWEISE

☒ Abbuchungsauftrag (siehe unten) ☐ Bankwechsel ☐ Kupons

☐ Scheck ☐ Barzahlung ☐ Sonstige *(einzeln angeben)*:

☐ Postanweisung ☐ Gebührenmarken

ABBUCHUNGSAUFTRAG *(diese Zahlungsweise gibt es nicht bei allen Anmeldeämtern)*

Das Anmeldeamt/ EP

☒ wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen.

☒ wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben.

☐ wird beauftragt, die Gebühr für die Ausstellung des Prioritätsbelegs und seine Übermittlung an das Internationale Büro der WIPO von meinem laufenden Konto abzubuchen.

28000629 23.10.1998 Dr. Andreas Schrell

Replaced by Article 34

Claims

1. A process for the digital signing of a message which is transmitted via a communication network to a signing unit and is to be signed, wherein the message to be signed is transmitted to the signing unit via a telephone network.

2. The process according to claim 1, wherein the signing unit is a mobile radio telephone.

3. The process according to any one of the preceding claims, wherein the message to be signed is transmitted from a transmitter to a receiver, this message is thereafter transmitted from the receiver via a telephone network, particularly a mobile-radio telephone network, to a mobile radio telephone associated with the transmitter, this message is then signed in the mobile radio telephone and retransmitted, as signed message, to the receiver.

4. The process according to any one of the preceding claims, wherein a public-key process is used for signing, particularly a public-key process in which the transmitter has an associated secret key and the receiver has a corresponding public key matching the secret key.

5. The process according to any one of the preceding claims, wherein the messages are transmitted between the receiver and the mobile radio telephone by means of the short-message service (SMS).

6. The process according to any one of the preceding claims, wherein, prior to signing, the message is displayed by means of a display provided in the mobile radio telephone.

7. The process according to any one of the preceding claims, wherein the secret key required for signing is inputted via keyboard means of the mobile radio telephone.

8. The process according to any one of the preceding claims, wherein the secret key required for signing is stored on a chipcard of the mobile radio telephone and this key is activated by means of a PIN adapted to be inputted via keyboard means of the mobile radio telephone.

9. The process according to any one of the preceding claims, wherein the chipcard carries out the generation of the signed message.

10. The process according to any one of the preceding claims, wherein the mobile radio telephone generates the signed message and wherein the secret key is read from the chipcard.

11. The process according to any one of the preceding claims, wherein the mobile radio telephone serves, in addition, as the sender for transmitting the signed message to the receiver.

12. Mobile radio telephone with a key pad, a display, and chipcard means for reading and/or writing a chipcard adapted to be inserted into the mobile radio telephone, characterised by signing means (21), particularly for generating a signed message (9) from a message (3) to be signed or/and for communicating with a chipcard (25) having signing means (21).

13. The mobile radio telephone according to claim 12, characterised in that the signing means (21) are connected with the key pad (19) for inputting a secret key or a secret number (PIN).

14. A chipcard for a mobile radio telephone, particularly according to claims 12 or 13, characterised in that the chipcard (25) comprises signing means (21) which include a memory unit (27) for storing the secret key required for generating the signed message (9).

15. The chipcard according to claim 14, characterised in that the chipcard (25) comprises signing means (21) which generate a signed message (9) from a message which is received by the mobile radio telephone and is to be signed.

is directly connected with the computer keyboard under exclusion of the computer software. The signature is generated in the signing unit. This process is the more cost-saving the fewer tasks must be carried out by the computer software and the lower the performance requirements to the signing unit.

However, in all this embodiments there is the basic problem that there must be signed precisely the data which the user wants to sign. It must be precluded that a virus affects the data, for example during the transmission from the display component, eg., from the display, to the signing component, eg., the cryptoprocessor. Furthermore, it must be ensured that a secret number (eg., the PIN), which is required to trigger signatures, cannot be read from the keyboard by other programs and does not become known to third parties.

Furthermore, the large-scale utilisation of the option of digital signing is limited by the comparatively small distribution of signing units. In fields of the potential application of digital signatures, eg., in internet banking, therefore a costly infrastructure would have to be set up to spread the use of signing units. Also the installation of signing units at the computer is problematic. On the one hand, the units must be physically connected to the computer, yet all the serial interfaces of a PC are often already in use. Alternative processes for incorporating signing units in computers are likewise problematic, since for this purpose software drivers and, sometimes, even additional hardware are required. Apart from this, for all signing units there must be implemented special software components which allow the user to communicate with the signing unit.

A further problem of the conventional processes for digital signatures results from the fact that they are location-dependent. Particular fields of application of digital signatures, eg., internet banking, are location-independent in view of the everywhere accessible public internet terminals. If these internet banking applications were combined with the known location-dependent processes for digital signing, the independence of the location would be lost in these applications.

A low-cost, easy-to-build, and location-independent process for the digital signing of communications and the provision of appropriate means are the technological problems underlying the present invention.

These technological problems are solved through the teachings according to the main claim. Thus, the invention creates a process for digital signing of a message which is transmitted via a communication network to a signing unit and is to be signed, with the message to be signed being transmitted to the signing unit via a telephone network. In a particularly preferred embodiment of the invention, the signing unit is a mobile radio telephone and, accordingly, the mobile phone network is the communication network.

In the context of the present invention, digital signing of a message is understood as a procedure in which the intent to deliver a message and its contents are confirmed electronically. This is effected by partial or full encoding of the message to be signed or by encoding of a cryptographic check sum of this message into a signed message by means of a secret key and by making use of an algorithm. In the context of the present invention, a signed message is understood either as the message as a whole or as the signature proper. Signing serves for being able to identify the user later on. In the context of the present invention, a signed message is understood also as merely the electronically generated signature of the message. In the context of the present invention, a message is understood as any kind of electronically reproducible information, for example, numbers, characters, combinations of numbers, combinations of characters, graphs, tables, etc. In the context of the present invention, a signing unit is understood as a unit which

Modified

Annex AU.IV

VERIFICATION OF TRANSLATION

I, Joachim Buchner,
(insert translator's name)

of Spruson & Ferguson, 31 Market Street,

Sydney, NSW, 2000, Australia
(translator's address)

declare as follows:

1. That I am well acquainted with both the English and German languages, and

2. That the attached document is a true and correct translation made by me to the best of my knowledge and belief of:-

(b) The Amendments made to the specification

International Application No. PCT/EP98/06769

April 27, 2000
(Date)

Joachim R. Büchner
(Signature of Translator)

(No witness required)

eab:914P

VERIFICATION OF TRANSLATION

I, Joachim Büchner,
(insert translator's name)

of Spruson & Ferguson, 31 Market Street, Sydney NSW 2000, Australia,
(translator's address)

declare as follows:

That I am well acquainted with both the English and German languages, and

2. That the attached document is a true and correct translation made by me to the best of my knowledge and belief of:-

(a) The specification of International Bureau pamphlet numbered

WO 99/22486

International Application No. PCT/EP98/06769

26/4/2000
(Date)

Joachim Büchner
(Signature of Translator)

(No witness required)

VE RAG ÜBER DIE INTERNATIONALE USAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
22738 WO			
Internationales Aktenzeichen	Internationales Anmeldedatum (Tag/Monat/Jahr)		(Frühestes) Prioritätsdatum (Tag/Monat/Jahr)
PCT/EP 98/06769	24/10/1998		28/10/1997
Anmelder			
BROKAT INFOSYSTEMS AG et al.			

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [X] wie vom Anmelder vorgeschlagen

   [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

AW

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/06769

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L H04Q G07B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 96 32700 A (AU SYSTEM ;JONSTROEMER ULF (SE)) 17. Oktober 1996 siehe Zusammenfassung siehe Seite 1-12 ---	1-4,6, 8-15
A	EP 0 689 316 A (AT & T CORP) 27. Dezember 1995 siehe Zusammenfassung siehe Spalte 1, Zeile 56 - Spalte 2, Zeile 28 siehe Spalte 9, Zeile 4 - Zeile 42 siehe Anspruch 1 siehe Abbildungen 1,3 --- -/--	1-15

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. März 1999	30/03/1999

Name und Postanschrift der internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

Internationales Aktenzeichen
PCT/EP 98/06769

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr
A	COMBANIERE C: "NOUVELLES POSSIBILIT S DE PAIEMENT" REE: REVUE GENERALE DE L ELECTRICITE ET DE L ELECTRONIQUE. Nr. 4. 1. Oktober 1995. Seiten 57-65. XP000533330 siehe das ganze Dokument ---	1-15
A	WO 97 37461 A (HEWLETT PACKARD CO ;MAO WENBO (GB)) 9. Oktober 1997 siehe Zusammenfassung siehe Seite 2, Zeile 23 - Seite 4, Zeile 25 siehe Seite 6, Zeile 23 - Seite 8, Zeile 15 siehe Anspruch 1 siehe Abbildungen 1-3 -----	1-15

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Ver... ...chungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 98/06769

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9632700 A	17-10-1996	SE 506506 C	22-12-1997
		NO 974626 A	13-10-1997
		SE 9501347 A	12-10-1996
EP 0689316 A	27-12-1995	CA 2149067 A	23-12-1995
		JP 8032575 A	02-02-1996
WO 9737461 A	09-10-1997	EP 0891663 A	20-01-1999